

Protected Critical Infrastructure Information (PCII) Program

Meghan Lutke

Chemical Security Summit

July 21-23, 2008



Homeland
Security

PCII Program Legislative History

The PCII Program is governed by the Critical Infrastructure Information (CII) Act of 2002 and the Final Rule:

- The CII Act is sections 211-215 of the Homeland Security Act of 2002 (6 U.S.C §§131-134)
- An Interim Final Rule established the PCII Program in February 2004
- The Final Rule: Procedures for Handling Critical Infrastructure Information was issued on September 1, 2006 (6 C.F.R. part 29)



PCII Program Overview

The PCII Program protects voluntarily submitted critical infrastructure information (CII) from public release through:

- Freedom of Information Act (FOIA)
- State and local disclosure laws
- Use in civil litigation

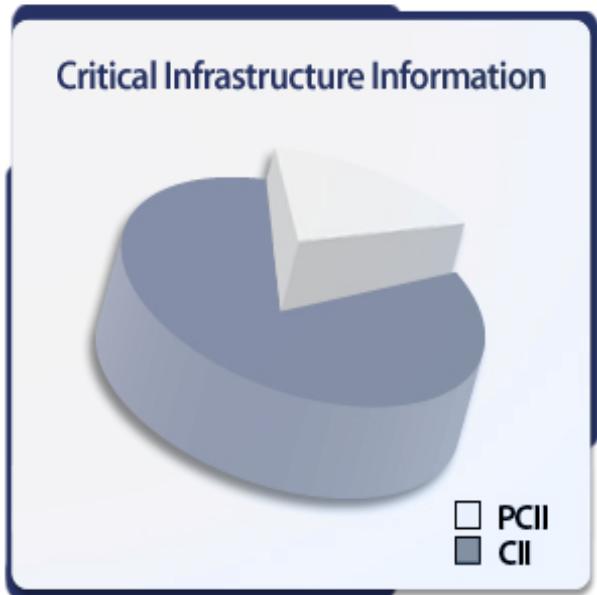
Additionally, PCII cannot be used for regulatory purposes



**Homeland
Security**

Examples of CII

The CII Act defines the following types of information as CII:



- **Threats**—Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of a critical asset
- **Vulnerabilities**—Ability to resist threats, including assessments or estimates of vulnerability
- **Operational experience**—Any past operational problem or planned or past solution including repair, recovery, or extent of incapacitation



**Homeland
Security**

User Access Requirements

PCII is made available to those Federal, State and local government employees and their contractors who:

- Are trained in the handling and safeguarding of PCII
- Have homeland security responsibilities
- Have a need to know the specific information
- Sign a Non-Disclosure Agreement (non-Federal employees)
- Are certified by the PCII Program Manager or PCII Officer (contractors)

E-mail training requests to pcii-training@dhs.gov



**Homeland
Security**

Safeguarding PCII

Safeguarding PCII is a shared responsibility between the PCII Program Office and government users to ensure:

- PCII is only accessed by authorized users with a need-to-know the information
- PCII is protected from inappropriate use
- PCII is disseminated appropriately
- Precautions are taken to prevent unauthorized persons from overhearing conversations, observing PCII materials or otherwise obtaining such information

PCII training and accreditation programs assist users and entities in applying PCII safeguarding requirements



**Homeland
Security**

Submission Process

Information may be voluntarily submitted to the PCII Program Office to be validated as PCII:

- By mail, fax, courier, or electronically through a secure Web portal at www.dhs.gov/pcii
- Through approved partnerships with DHS field representatives or other Federal agencies

Submissions must include:

- An Express Statement stating the information is voluntarily submitted and requesting the protections of the CII Act
- A Certification Statement stating the information is not customarily in the public domain, and the submitter's contact information



**Homeland
Security**

Program Participation

Federal

- Two Federal entities accredited
- Three Federal entities in process

State

- 12 State entities accredited
- 33 State entities in process

Information-Collection Partnerships

- Five DHS partnerships
- Partnerships in development with other Federal entities to include DoD



**Homeland
Security**

Additional Information

For additional information on the PCII Program:

- Website: www.dhs.gov/pcii
- Email: Pcii-info@dhs.gov
- Phone: 202-360-3023



**Homeland
Security**